MINISTÉRIO DA DEFESA

MD31-M-07

Doutrina Militar de Defesa Cibernética

2023

MINISTÉRIO DA DEFESA
ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS

Doutrina Militar de Defesa Cibernética

2ª Edição
2023

MINISTÉRIO DA DEFESA
ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS

Portaria GM-MD n° 5.081, de 16 de outubro de 2023

Aprova a Doutrina Militar de Defesa Cibernética - MD31-M-07 (2ª Edição/2023).

O **MINISTRO DE ESTADO DA DEFESA**, no uso das atribuições que lhe confere o art. 87, parágrafo único, inciso I, da Constituição, tendo em vista o disposto no art. 1º, inciso III, do Anexo I, do Decreto nº 11.337, de 1º de janeiro de 2023, e de acordo com o que consta do Processo Administrativo nº 60080.000234/2023-31 resolve:

Art. 1º Esta Portaria aprova a Doutrina Militar de Defesa Cibernética - MD31-M-07 (2ª Edição/2023), na forma do Anexo.

Parágrafo único. O teor da Doutrina de que trata o **caput** estará disponível na Assessoria de Doutrina e Legislação - ADL do Estado-Maior Conjunto das Forças Armadas - EMCFA e na Plataforma de Pesquisa da Legislação da Defesa - MDLegis (<https://mdlegis.defesa.gov.br/pesquisar_normas/>).

Art. 2º Fica revogada a Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014, publicada no Diário Oficial da União nº 224, de 19 de novembro de 2014, Seção 1, página 9.

Art. 3º Esta Portaria entra em vigor em 1º de novembro de 2023.

JOSÉ MUCIO MONTEIRO FILHO

(Publicado no DOU, Edição nº 203, de 25 de outubro de 2023)

REGISTRO DE MODIFICAÇÕES

NÚMERO DE ORDEM	ATO DE APROVAÇÃO	PÁGINAS AFETADAS	DATA	RUBRICA DO RESPONSÁVEL

SUMÁRIO

LISTA DE DISTRIBUIÇÃO

INTERNA	
ÓRGÃOS	**EXEMPLARES**
CHEFIA DE OPERAÇÕES CONJUNTAS	1
CHEFIA DE ASSUNTOS ESTRATÉGICOS	1
CHEFIA DE LOGÍSTICA E MOBILIZAÇÃO	1
CHEFIA DE EDUCAÇÃO E CULTURA	1
ASSESSORIA DE INTELIGÊNCIA DE DEFESA	1
ASSESSORIA DE DOUTRINA E LEGISLAÇÃO - **Exemplar Mestre**	1
PROTOCOLO GERAL	1
SUBTOTAL	**7**

EXTERNA	
ÓRGÃOS	**EXEMPLARES**
ESTADO-MAIOR DA ARMADA	1
ESTADO-MAIOR DO EXÉRCITO	1
ESTADO-MAIOR DA AERONÁUTICA	1
COMANDO DE OPERAÇÕES NAVAIS	1
COMANDO DE OPERAÇÕES TERRESTRES	1
COMANDO DE OPERAÇÕES AEROESPACIAIS	1
SUBTOTAL	**6**
TOTAL	**13**

CAPÍTULO I

INTRODUÇÃO

1.1 Finalidades

Estabelecer os fundamentos da Doutrina Militar de Defesa Cibernética, proporcionar unidade de pensamento sobre o assunto, no âmbito da Defesa Nacional, e contribuir para a atuação conjunta das Forças Armadas (FA) na defesa do Espaço Cibernético de Interesse do Brasil.

1.2 Referências

Os documentos consultados e que fundamentaram a elaboração desta publicação foram:

a) Constituição da República Federativa do Brasil, de 1988;

b) Lei Complementar (LC) nº 97, de 9 de junho de 1999 (dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas);

c) Lei nº 12.965, de 23 de abril de 2014 (estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil);

d) Projeto Decreto Legislativo nº 1.127/2021 (aprova os textos da Política Nacional de Defesa- PND, da Estratégia Nacional de Defesa- END e do Livro Branco de Defesa Nacional- LBDN, encaminhados ao Congresso Nacional pela Mensagem (CN) nº 9, de 2020 (Mensagem nº 398, de 16 de julho de 2020, na origem);

e) Decreto nº 7.276, de 25 de agosto de 2010 (aprova a Estrutura Militar de Defesa e dá outras providências);

f) Decreto nº 11.331, de 1º de janeiro de 2023 (define as competências do DSIC – GSI/PR, dentre outras);

g) Decreto nº 7.809, de 20 de setembro de 2012 (altera a estrutura regimental da Marinha, do Exército e da Aeronáutica);

h) Decreto nº 9.573, de 22 de novembro de 2018 (institui a Política Nacional de Segurança de Infraestruturas Críticas – PNSIC);

i) Decreto nº 9.637, de 26 de dezembro de 2018 (institui a Política Nacional de Segurança da Informação – PNSI);

j) Decreto nº 10.222, de 05 de fevereiro de 2020 (aprova a Estratégia Nacional de Segurança Cibernética - E-Ciber);

k) Decreto nº 10.569, de 9 de dezembro de 2020 (aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas - ENSIC);

l) Decreto nº 10.748, de 16 de julho de 2021 (institui a Rede Federal de Gestão de Incidentes Cibernéticos);

m) Decreto nº 11.200, de 15 de setembro de 2022 (aprova o Plano Nacional de Segurança de Infraestruturas Críticas);

n) Decreto nº 11.491, de 12 de abril de 2023 (promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001);

o) Decreto nº 10.748, de 16 de julho de 2021 (institui a Rede Federal de Gestão de Incidentes Cibernéticos no âmbito da administração pública federal);

p) Portaria GSI/PR nº 93, de 18 de outubro de 2021 (aprova o Glossário de Segurança da

Informação);

q) Portaria Normativa nº 9/GAP/MD, de 13 de janeiro de 2016 (aprova o Glossário das Forças Armadas – MD35- G-01, 5ª Edição);

r) Portaria GM/MD nº 4.034, de 1º de outubro de 2021 (aprova o Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas - MD33-M-02, 4ª Edição/2021);

s) Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012 (aprova a Política Cibernética de Defesa - MD31-P-02 - 1ª Edição/2012);

t) Portaria Normativa nº 32/MD, de 30 de agosto de 2017 (aprova a publicação Operações Interagências - MD33-M-12, 2ª Edição/2017);

u) Portaria Normativa nº 84/GM/MD, de 15 de setembro de 2020 (aprova a Doutrina de Operações Conjuntas - MD30-M-01, Volumes 1 e 2 - 1ª Edição/2020);

v) Portaria GSI/PR nº 93, de 18 de outubro de 2021 (aprova o Glossário de Segurança da Informação);

x) Diretriz Ministerial nº 14/2009 do Ministério da Defesa, de 9 de novembro de 2009 (dispõe sobre integração e coordenação dos setores estratégicos da Defesa);

y) Instrução Normativa EMCFA/MD nº 3, de 14 de junho de 2022 (aprova as Instruções para Elaboração e Revisão de Publicações Padronizadas do Estado-Maior Conjunto das Forças Armadas - MD20-I-01, 2ª Edição/2022);

z) Portaria Normativa nº 2.777/MD, de 27 de outubro de 2014 (dispõe sobre a diretriz de implantação de medidas visando à potencialização da defesa cibernética nacional e dá outras providências);

aa) Portaria nº 001, de 2 de janeiro de 2015 (cria o Comando de Defesa Cibernética e dá outras providências);

ab) Portaria nº 002, de 2 de janeiro de 2015 (cria a Escola Nacional de Defesa Cibernética e dá outras providências);

ac) Portaria nº 219-EME, de 30 de maio de 2017 (aprova a Diretriz de Implantação do ComDCiber);

ad) Portaria nº 3.781/GM-MD, de 17 de novembro de 2020 (cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências; e

ae) Portaria nº 4.138/GM-MD, de 14 de agosto de 2023 (institui a Equipe de Coordenação Setorial da Defesa- ECS/Def da Rede Federal de Gestão de Incidentes Cibernéticos- ReGIC).

1.3 Considerações iniciais

1.3.1 Após a publicação da primeira edição desta Doutrina, em novembro de 2014, houve uma evolução da maturidade do setor cibernético da defesa nacional a partir da criação do Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber), em janeiro de 2015, logo após a criação do Programa Defesa Cibernética na Defesa Nacional (PDCDN). O ano de 2016 foi marcado pela ativação do ComDCiber, pelo reconhecimento do espaço cibernético como domínio operacional por parte da Organização do Tratado do Atlântico Norte (OTAN) e pela primeira participação de uma Força Conjunta de Guerra Cibernética (F Cj G Ciber) em uma operação conjunta organizada pelo Estado-Maior Conjunto das Forças Armadas (EMCFA).

1.3.2 A partir de 2017, a Defesa Cibernética deu mais um passo na sua evolução com a participação do ComDCiber em operações nacionais e internacionais e pela sua caracterização como Comando

Conjunto, haja vista a designação de oficiais generais das três Forças Armadas para compor seus quadros.

1.3.3 Outro fato relevante para o Sistema Militar de Defesa Cibernética (SMDC) foi a publicação do Decreto nº 9.637/2018, o qual instituiu a Política Nacional de Segurança da Informação (PNSI), incluindo a Segurança Cibernética e a Defesa Cibernética na abrangência da Segurança da Informação em âmbito nacional.

1.3.4 O Decreto nº 10.222/2020, aprovou a Estratégia Nacional de Segurança Cibernética (E-Ciber) com os objetivos estratégicos de tornar o Brasil mais próspero e confiável no ambiente digital; aumentar a resiliência brasileira às ameaças cibernéticas; e fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

1.3.5 O Decreto nº 10.569/2020 aprovou a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), e estabeleceu que as infraestruturas de comunicações, energia, transportes, finanças e águas, dentre outras, possuem dimensão estratégica, uma vez que desempenham papel essencial tanto para a segurança e soberania nacionais, como para a integração e o desenvolvimento econômico sustentável do País.

1.3.6 O Plano Nacional de Segurança de Infraestruturas Críticas (PNSIC) conta com mecanismos de acompanhamento da execução das ações e do atingimento de metas, destacando: os Eixos Estruturantes; a Gestão de Dados e Informações; o incentivo à adoção de recursos e de procedimentos voltados para a segurança cibernética nas infraestruturas críticas; o estímulo aos responsáveis pelas infraestruturas críticas para ampliarem seus investimentos em recursos cada vez mais avançados de segurança cibernética; e a atenção às ações estratégicas E-Ciber no que se refere à proteção das Infraestruturas Críticas Nacionais.

1.3.7 O capítulo 2 deste manual aborda os fundamentos da capacidade cibernética, apresentando aspectos evolutivos da doutrina em outros países e seus reflexos na doutrina brasileira. No capítulo 3, detalha-se a estrutura e o funcionamento do SMDC, mantendo coerência com a atualização da Doutrina de Operações Conjuntas. A estrutura do ComDCiber encontra-se no capítulo 4, facilitando a compreensão das funções de cada componente do Comando no contexto do SMDC. Por fim, o capítulo 5 (Capacidade Cibernética em Operações) descreve os aspectos doutrinários mais relevantes para o emprego militar neste novo ambiente operacional.

1.3.8 O disposto nesta doutrina, no que toca ao emprego da capacidade cibernética em todo o espectro dos conflitos, ativado ou não um(a) Teatro de Operações/ Área de Operação (TO/A Op), será regulado/complementado por meio das Normas Operacionais do Sistema Militar de Defesa Cibernética (NOSDCiber), aprovadas pelo Chefe do Estado-Maior Conjunto das Forças Armadas (CEMCFA), mediante proposta do ComDCiber.

1.3.9 Durante o período de normalidade, em atenção ao Decreto nº 10.748/2021 que instituiu a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) no âmbito da administração pública federal, foi criada a Equipe de Coordenação Setorial da Defesa (ECS/Def) por intermédio da Portaria GM-MD nº 4.138/2023, do Ministério da Defesa. Esta Equipe, operada pelo ComDCiber, tem por missão coordenar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no âmbito do Setor Defesa, consolidando as notificações dos principais incidentes cibernéticos das

equipes centrais do Ministério da Defesa, das Forças Singulares e das demais Equipes de Prevenção, Tratamento e Resposta a Incidentes em Redes (ETIR) públicas ou privadas relacionadas ao setor Defesa. Cabe ressaltar que esta estrutura permanecerá em operação mesmo durante o acionamento do Teatro de Operações (TO).

1.3.10 O Brasil, na esteira dos acontecimentos relevantes ocorridos no espaço cibernético nos últimos anos, também reconhece esse ambiente como um domínio operacional, no qual ações cibernéticas ofensivas e defensivas tendem a potencializar ou complementar as ações realizadas nos demais domínios (terra, mar, ar e espaço).

1.3.11 Dessa forma, esta atualização da doutrina busca refletir as mudanças ocorridas desde a aprovação da edição anterior, ao mesmo tempo em que busca ampliar a compreensão dos empregos estratégico, operacional e tático do espaço cibernético em proveito da Defesa Nacional.

1.4 Aplicação

Esta doutrina aplica-se ao Ministério da Defesa e aos Comandos da Marinha, do Exército e da Aeronáutica, devendo ser observada por ocasião da elaboração ou da reedição de outras publicações relacionadas ao assunto.

1.5 Informação

As abreviaturas utilizadas nesta publicação seguem o previsto no Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas – MD33-M-02 (4ª edição/2021). As abreviaturas, acrônimos e siglas não previstos no citado Manual farão parte de uma lista, em anexo.

1.6 Aprimoramento

1.6.1 A atualização desta doutrina será realizada em 2026, ou mesmo previamente, dada a rápida evolução na área de cibernética.

1.6.2 As sugestões para aperfeiçoamento deste documento deverão ser encaminhadas ao Estado-Maior Conjunto das Forças Armadas (EMCFA), via cadeia de comando, para o seguinte endereço:

MINISTÉRIO DA DEFESA
Estado-Maior Conjunto das Forças Armadas
Assessoria de Doutrina e Legislação
Esplanada dos Ministérios
Bloco Q (Edifício Defensores da Pátria) – 4º Andar
Brasília – DF
CEP – 70049-900
adl.emcfa@defesa.gov.br

CAPÍTULO II

FUNDAMENTOS

2.1 Considerações Iniciais

2.1.1 Depois do estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa (END), em 2008, três campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República (PR); a Defesa Cibernética, a cargo do Ministério da Defesa; e a Guerra Cibernética, a cargo dos Comandos Operacionais ativados e de suas Forças Componentes.

2.1.2 O espaço cibernético nacional é composto pelos seguintes níveis de decisão e atores (conforme apresentado na figura 1):

a) Nível Político: Segurança Cibernética, coordenado pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), abrangendo a Administração Pública Federal (APF) e as Infraestruturas Críticas (IC);

b) Nível Estratégico: Defesa Cibernética, a cargo do Ministério da Defesa (MD), do Estado-Maior Conjunto das Forças Armadas (EMCFA) e dos Comandos das Forças Armadas (FA), interagindo com o GSI/PR, APF, agências e IC de interesse para a Defesa Nacional; e

c) Níveis Operacional e Tático: Guerra Cibernética, a cargo dos Comandos Operacionais ativados e das Forças Componentes.
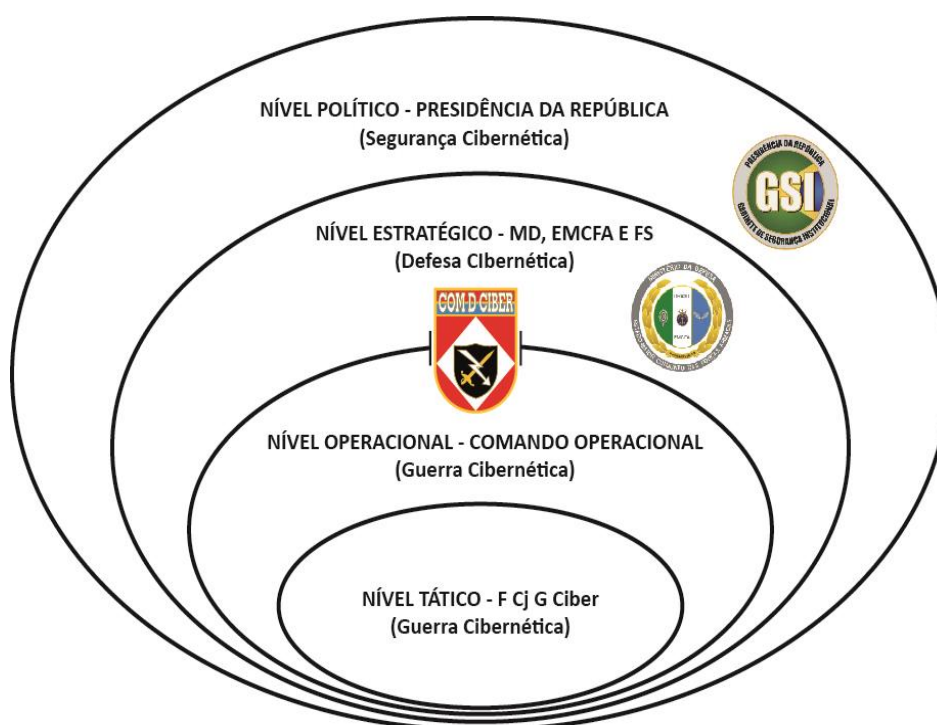
Figura 1 – Níveis de decisão e atores no espaço cibernético

2.1.3 Em conformidade com o item anterior, será utilizada a denominação Defesa Cibernética quando do planejamento e da execução de ações cibernéticas afetas ao nível estratégico de decisão. Da mesma forma, será utilizada a denominação Guerra Cibernética quando o nível de decisão considerado for operacional ou tático.

2.2 Conceitos

2.2.1 Acrescentam-se aos conceitos já definidos no Glossário das Forças Armadas (MD35-G-01, 5ª Edição) e no Glossário de Segurança da Informação (Portaria nº 93/GSI-PR, de 18 de outubro de 2021) os seguintes termos:

2.2.1.1 Acesso Cibernético - ato de interagir ou usar os ativos de informação no Espaço Cibernético de Interesse.

2.2.1.2 Ações Cibernéticas - ações realizadas no espaço cibernético por pessoal especializado e com o emprego de tecnologias e processos específicos, que visam contribuir para a consecução de objetivos militares.

2.2.1.3 Ameaça Cibernética - causa potencial de um incidente indesejado que pode resultar em dano ao espaço cibernético de Interesse.

2.2.1.4 Artefato Cibernético - equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataques cibernéticos.

2.2.1.5 Ativos de informação - meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e interconexão), os sistemas utilizados para tal, os sistemas de informação de um modo geral, bem como os locais onde se encontram esses meios e os recursos humanos que a eles têm acesso.

2.2.1.6 Capacidade Cibernética (Cpcd Ciber) - ~~é~~ a aptidão para emprego de ações cibernéticas implementadas para criar efeito no espaço cibernético ou por meio dele.

2.2.1.7 Centro de Gravidade Cibernético (CG Ciber) - A identificação dos Centros de Gravidade no Espaço Cibernético de Interesse é fundamental durante o planejamento, tanto em operações cibernéticas defensivas quanto ofensivas. Entende-se por CG Ciber a porção do Espaço Cibernético de Interesse cuja conquista ou manutenção confere uma posição vantajosa a seu ocupante, em última análise, a liberdade de ação para utilizar integralmente seu poder de combate. O CG Ciber, uma vez conquistado ou atingido, poderá resultar no comprometimento da estrutura de redes e sistemas, uma vez que se trata de um ou mais ativos da informação críticos para o funcionamento destes.

2.2.1.8 Cibernética - termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e suas interações. No campo da Defesa Nacional, inclui os recursos de Tecnologia da Informação e Comunicações (TIC) de cunho estratégico, tais como aqueles que compõem o Sistema Militar de

Comando e Controle (SISMC²), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais.

2.2.1.9 Ciberpersona - representação da identidade virtual de uma pessoa ou uma instituição no espaço cibernético. Uma pessoa ou instituição pode ter múltiplas identidades virtuais, assim como mais de uma pessoa ou instituição podem compartilhar uma única identidade.

2.2.1.10 Defesa Cibernética - ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente.

2.2.1.11 Espaço Cibernético – espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.

2.2.1.12 Espaço Cibernético de Interesse (Espç Ciber Intrs) – Parcela do espaço cibernético onde os fatores e acontecimentos que nele se produzam possam repercutir no resultado ou afetar as ações, cinéticas ou não, atuais e futuras de um Teatro de Operações (TO) ou de uma Área de Interesse.

2.2.1.13 Espaço Cibernético do Sistema Militar de Defesa Cibernética (Espç Ciber SMDC) - Ambiente informacional de interesse do SMDC composto pelos ativos de informação do MD, das Forças Armadas e dos Comandos Operacionais ativados, assim como de outros órgãos eventualmente incluídos no Sistema, que necessitam ser protegidos das ameaças cibernéticas.

2.2.1.14 Superfície de Ataque Cibernético – conjunto de ativos de informação de um espaço cibernético expostos publicamente na Internet às ações ofensivas cibernéticas ou dispostos em uma rede interna de conhecimento de uma ameaça cibernética.

2.3 Base Conceitual de Emprego

2.3.1 Relação do espaço cibernético com os Domínios Operacionais - Embora faça parte do ambiente informacional, o espaço cibernético interage transversalmente com os domínios operacionais aéreo, terrestre, marítimo e espacial.

a) As operações cibernéticas dependem de infraestruturas de TI, sejam elas ligadas em rede, autônomas, em nuvem ou embarcadas em plataformas aéreas, terrestres e marítimas. Usam enlaces e nós localizados nos domínios operacionais e executam funções lógicas para criar efeitos, primeiro no espaço cibernético e, conforme necessário, nos domínios operacionais; e

b) Essas operações, através de um meticuloso controle dos efeitos, podem fornecer liberdade de ação para atividades nos demais domínios operacionais.

2.3.2 Operações Cibernéticas (Op Ciber) – aquelas onde o emprego de ações cibernéticas busca, principalmente, atingir objetivos e efeitos no espaço cibernético ou por meio dele.

2.3.2.1 Cada Operação Cibernética é classificada dentro de uma das duas missões no espaço cibernético:

a) Operações Cibernéticas Defensivas (Op Ciber Def); ou

b) Operações Cibernéticas Ofensivas (Op Ciber Ofs).

2.3.3 A classificação das missões em uma das categorias acima é realizada exclusivamente com base na intenção ou objetivo da autoridade responsável e não se baseia nas ações cibernéticas executadas, nas forças atribuídas à missão ou nas capacidades cibernéticas utilizadas.

2.3.4 As Op Ciber são conduzidas para obter ou manter a liberdade de ação no ciberespaço, cumprir os objetivos operacionais estabelecidos, negar a liberdade de ação à ameaça e permitir outras atividades operacionais.

2.3.5 Operações Cibernéticas Defensivas (Op Ciber Def) - têm por objetivo neutralizar a ameaça de um oponente específico e/ou retornar uma rede comprometida a um estado seguro e funcional. As Op Ciber Def devem ser direcionadas de acordo com a priorização dos ativos de informação no espaço cibernético. As Op Ciber Def se subdividem em:

a) Medidas de Defesa Interna (MDI); e

b) Ações de Resposta (Aç Rsp).

2.3.6 Medidas de Defesa Interna (MDI) - constituem uma forma de Op Ciber Def que ocorrem dentro da porção do espaço cibernético a ser defendido. São autorizadas por meio de ordens observando-se o arcabouço jurídico vigente. Incluem ações cibernéticas defensivas para confirmar ou restabelecer a segurança de uma porção do espaço cibernético de uma das redes que tenha sido degradada, comprometida ou de alguma outra maneira ameaçada, de modo a estabelecer um nível de acesso suficiente para garantir o prosseguimento das operações militares. A maioria das Op Ciber Def são MDI, as quais incluem busca proativa por ameaças avançadas e/ou persistentes, bem como contramedidas e respostas internas ativas para eliminar essas ameaças e mitigar seus efeitos. São exemplos de efeitos das MDI no espaço cibernético:

a) Isolamento: bloquear a(s) linha(s) de comunicação entre o adversário e os sistemas afetados;

b) Contenção: impedir que a atividade maliciosa amplie seu alcance;

c) Neutralização: tornar a atividade maliciosa permanentemente incapaz de continuar afetando as partes dos sistemas informacionais; e

d) Recuperação: remover e mitigar os efeitos da atividade maliciosa em sistemas afetados de forma a restaurar sua funcionalidade.

2.3.7 Ações de Resposta (Aç Rsp) - são uma forma de Op Ciber Def na qual as ações tomadas são externas à porção do espaço cibernético defendido. Algumas Op Ciber Def – Aç Rsp podem incluir ações que caracterizem o uso da força, com danos físicos ou destruição de sistemas do oponente, dependendo do contexto operacional mais amplo, tal como a existência ou iminência de hostilidades abertas, o nível de certeza na atribuição da ameaça, o dano que a ameaça pode causar e considerações de política nacional.

2.3.8 Operações Cibernéticas Ofensivas (Op Ciber Ofs) - têm por objetivo projetar poder no Espaço Cibernético de Interesse por meio de ações tomadas em apoio aos Comandos Operacionais ou objetivos nacionais definidos por arcabouço jurídico vigente. Os seguintes efeitos podem ser obtidos por meio de Op Ciber Ofs:

a) Manipulação: controlar, mudar ou comprometer a integridade de informações, sistemas e/ou redes adversárias, de modo a apoiar os objetivos do Comando;

b) Exfiltração: reunir, transferir, publicar ou obter a posse de informação através de acesso não-autorizado;

c) Degradação: negar acesso ou a operação de um ativo através da redução do nível de sua capacidade ou desempenho. O nível de redução desejado normalmente é especificado pela autoridade requisitante;

d) Interrupção: negar acesso ou a operação de um ativo por um período de tempo. Normalmente, a hora de início e de término da interrupção são especificadas pela autoridade requisitante. A interrupção pode ser considerada como um caso especial de degradação, no qual o nível selecionado é de 100% durante o tempo determinado; e

e) Destruição: negar acesso ou a operação de um ativo completamente e de forma irreparável. O ativo é afetado em máxima extensão, tanto em termos de tempo de indisponibilidade quanto de danos causados.

2.3.9 As Op Ciber Ofs alcançam efeitos no Espaço Cibernético de Interesse ou ativam efeitos em cascata nos domínios físicos que afetem sistemas de armas, processos de C^2, nós logísticos, alvos de alto valor, dentre outros objetivos do inimigo, além de contribuir para os objetivos informacionais estabelecidos.

2.3.10 Aumento da Resiliência do espaço cibernético não pertencente ao SMDC - as Op Ciber Def geralmente focam nos ativos do SMDC. Entretanto, as ações cibernéticas podem proteger qualquer outra porção do espaço cibernético nacional, uma vez que as operações militares dependem de outros segmentos do espaço cibernético, incluindo aqueles da iniciativa privada, e de outras agências governamentais.

2.3.11 Quando necessário e autorizado, mediante coordenação com o GSI/PR, MD e outros ministérios e agências, as FA e o ComDCiber contribuirão para a proteção de outras infraestruturas críticas e recursos-chave nacionais.

2.3.12 Para as Op Ciber, acesso cibernético significa um nível suficiente de visibilidade, conectividade ou ingresso a um dispositivo, sistema ou rede de modo a permitir futuras operações.

2.3.13 A sincronização e coordenação do acesso ao Espaço Cibernético de Interesse daqueles que se utilizam dele é vital para realização de Op Ciber. É fator crítico para o sucesso das operações de todos os tipos. A falta de sincronização pode acarretar resultados negativos não apenas à Defesa, mas também a outros setores que são de interesse da Defesa Nacional.

2.3.14 Camadas do Espaço Cibernético de Interesse das Operações Cibernéticas - para auxiliar no planejamento e execução das Op Ciber, o espaço cibernético pode ser descrito em três camadas inter-relacionadas:

a) Camada Física;
b) Camada Lógica; e
c) Camada de Ciberpersona.
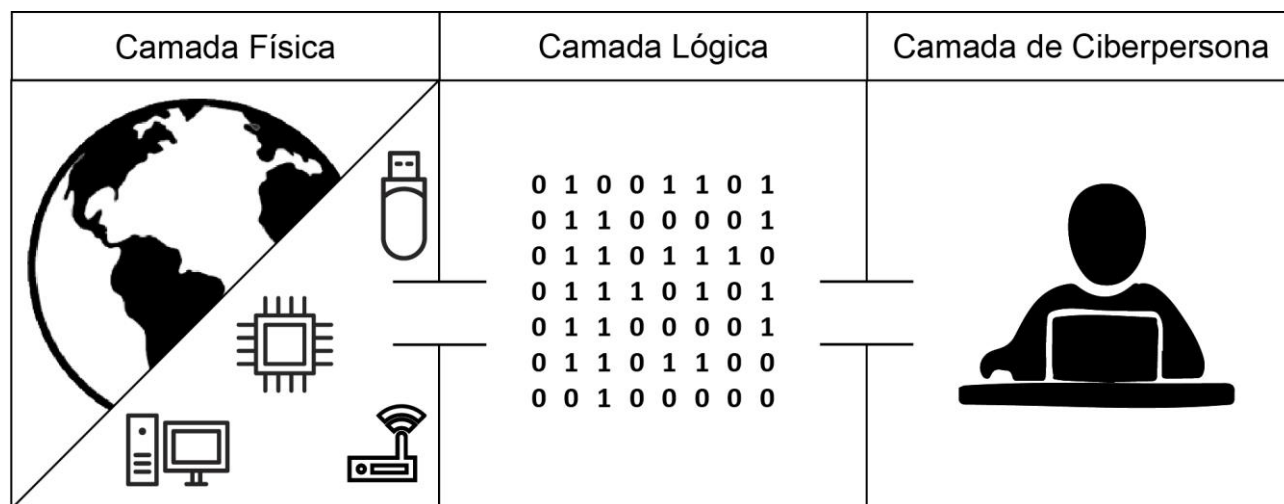
Figura 2 – Camadas do espaço cibernético

2.3.15 Cada camada representa um foco diferente, a partir do qual as Op Ciber podem ser planejadas, conduzidas e avaliadas.

2.3.16 Camada Física - formada pelos dispositivos e infraestrutura de Tecnologia de Informação (TI) que fornecem armazenamento, transporte e processamento da informação dentro do espaço cibernético, incluindo repositórios de dados e as conexões que transferem os dados entre os componentes. Os componentes da rede física incluem o *hardware* e a infraestrutura (dispositivos de computação, armazenamento, rede, além de enlaces cabeados e sem fio).

2.3.17 Os componentes dessa camada estão ligados a uma localização geográfica. O conhecimento dessa localização permite determinar o enquadramento legal apropriado para as ações, além de esclarecer questões de soberania ligadas aos domínios físicos.

2.3.18 Camada Lógica - Abstração da camada física podendo ser representada por aplicações, programas, serviços, protocolos que possibilitam o funcionamento e o tráfego de dados no espaço cibernético.

2.3.19 Alvos na camada lógica somente podem ser engajados através do uso de uma capacidade cibernética.

2.3.20 O modo de atuação na camada lógica é o diferencial das Op Ciber, pois visam obter efeitos no espaço cibernético ou por meio dele.

2.3.21 Camada de Ciberpersona - camada formada pelas representações das identidades virtuais dos usuários da rede (ciberpersonas). Essas identidades virtuais podem ser uma conta em um serviço online.

2.3.22 O uso de ciberpersonas pode tornar a atribuição de responsabilidades pelas ações cibernéticas difícil, fator preponderante que caracteriza a complexidade dessa camada, com elementos em muitas localizações virtuais que não compartilham uma única localização ou forma física. Desse modo, sua identificação requer uma considerável coleta e análise de Inteligência para permitir uma seleção de alvos efetiva ou para criar o efeito desejado dentro do contexto de uma operação militar.

2.3.23 Visualização do espaço cibernético baseado na localização e propriedade.

As porções do espaço cibernético podem ser classificadas em:

a) Espaço Cibernético Azul: são as áreas no espaço cibernético protegidas pelo SMDC, além de outras áreas as quais o MD receba a atribuição de proteger;

b) Espaço Cibernético Vermelho: porções do espaço cibernético pertencentes ou controladas pelo oponente ou força adversa. Entende-se por controladas não somente a presença oculta na rede, mas a capacidade de conduzir ações no espaço cibernético que exclua outros usuários; e

c) Espaço Cibernético Cinza: engloba todo o restante do espaço cibernético de interesse não enquadrado na descrição do espaço cibernético azul ou vermelho.

2.4 Princípios de Emprego da Defesa Cibernética

2.4.1 As operações militares, incluindo as realizadas no espaço cibernético, guiam-se pelos princípios listados na Doutrina Militar de Defesa. As peculiaridades da Defesa Cibernética impõem, ainda, que outros princípios relevantes sejam considerados.

2.4.2 São princípios de emprego da Defesa Cibernética:

a) Adaptabilidade;
b) Dissimulação;
c) Efeito; e
d) Rastreabilidade

2.4.3 Princípio da Adaptabilidade - consiste na capacidade da Defesa Cibernética de adaptar-se à característica de mutabilidade do espaço cibernético, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis.

2.4.4 Princípio da Dissimulação - medidas ativas e passivas devem ser adotadas para dificultar a rastreabilidade das ações cibernéticas ofensivas. Objetiva-se, assim, mascarar a autoria e o ponto de origem dessas ações.

2.4.5 Princípio do Efeito - as ações no espaço cibernético devem produzir efeitos cinéticos ou não cinéticos que contribuam para a consecução dos objetivos militares.

2.4.6 Princípio da Rastreabilidade - medidas efetivas devem ser adotadas para se detectar ações cibernéticas ofensivas e exploratórias contra o próprio Espç Ciber Intrs.

2.5 Características da Defesa Cibernética

2.5.1 Além de atender aos seus princípios de emprego e aos princípios de guerra, a Defesa Cibernética apresenta as seguintes características:

a) Insegurança Latente;
b) Alcance Global;
c) Vulnerabilidade das Fronteiras Geográficas;
d) Mutabilidade;
e) Incerteza;
f) Dualidade;
g) Paradoxo Tecnológico;
h) Dilema de Segurança; e
i) Assimetria.

2.5.2 Insegurança Latente - nenhum sistema computacional é totalmente seguro, na medida que as vulnerabilidades nos ativos de informação estão sempre sujeitas às ameaças cibernéticas.

2.5.3 Alcance Global - a Defesa Cibernética possibilita a condução de ações em escala global, simultaneamente, em diferentes frentes. Limitações físicas de distância e espaço não se aplicam ao espaço cibernético.

2.5.4 Vulnerabilidade das Fronteiras Geográficas - as ações cibernéticas não se limitam às fronteiras geograficamente definidas, pois os agentes podem atuar a partir de qualquer local e provocar efeito em qualquer lugar.

2.5.5 Mutabilidade - não existem leis de comportamento imutáveis no espaço cibernético, pois as ações cibernéticas podem adaptar-se às condições ambientais e à criatividade do ser humano.

2.5.6 Incerteza - as ações cibernéticas podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados.

2.5.7 Dualidade - na Defesa Cibernética, as mesmas ferramentas podem ser usadas de forma ofensiva ou defensiva com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas alvos e, por administradores, para descobrir as fraquezas de equipamentos e redes.

2.5.8 Paradoxo Tecnológico - quanto maior é o desenvolvimento tecnológico, maior é a dependência da TI e, consequentemente, maior a vulnerabilidade às ações cibernéticas. Contudo, paradoxalmente, melhores são as condições de defesa face a ataques cibernéticos em virtude do alto grau de desenvolvimento tecnológico.

2.5.9 Dilema de Segurança - dúvida que o gestor dos ativos de informação de uma Força enfrenta sobre a busca ou não da correção de uma vulnerabilidade identificada em um determinado sistema, uma vez que a correção tornará mais eficiente a sua defesa, enquanto a não correção aumenta a capacidade de ataque a sistemas congêneres de posse de um eventual oponente.

2.5.10 Assimetria - baseada no desbalanceamento de forças, causada pela introdução de um ou mais elementos de ruptura tecnológicos, metodológicos ou procedimentais que podem vir a causar danos tão prejudiciais quanto aqueles perpetrados por Estados ou organizações com maiores condições econômicas, por exemplo.

2.6 Possibilidades da Defesa Cibernética

2.6.1 São possibilidades da Defesa Cibernética:

a) atuar no espaço cibernético, por meio de ações ofensivas e defensivas;

b) cooperar na produção do conhecimento de Inteligência por meio da Fonte Cibernética;

c) atingir as infraestruturas críticas de um oponente, por meio de seus ativos de informação, sem limitação de alcance físico e exposição de tropa;

d) contribuir com a manobra informacional de uma operação, em coordenação com outras capacidades relacionadas à informação;

e) cooperar com a Segurança Cibernética, inclusive, de órgãos externos ao MD, mediante solicitação ou no contexto de uma operação;

f) cooperar com o esforço de mobilização para assegurar a capacidade dissuasória cibernética;

g) obter a surpresa com mais facilidade, baseado na capacidade de explorar as vulnerabilidades dos sistemas de informação do oponente;

h) realizar ações contra oponentes mais fortes, dentro do conceito de guerra assimétrica; e

i) realizar ações com custos significativamente menores que as operações militares nos demais domínios.

2.7 Peculiaridades importantes da Defesa Cibernética

2.7.1 São peculiaridades importantes da Defesa Cibernética:

a) dificuldade para identificar o agente da ação no domínio cibernético (atribuição);

b) constante identificação de novas vulnerabilidades nos sistemas computacionais;

c) dificuldade de identificação e retenção de talentos humanos;

d) grande vulnerabilidade a ações de oponentes com poder assimétrico;

e) dificuldade de acompanhamento da evolução tecnológica; e

f) dificuldade de identificação e mitigação das vulnerabilidades dos próprios sistemas de informação.

2.8 Formas de atuação cibernética

2.8.1 As formas de atuação cibernética podem variar de acordo com o nível dos objetivos (político, estratégico, operacional ou tático), nível de envolvimento nacional, contexto de emprego, nível tecnológico empregado, sincronização e tempo de preparação.

2.8.2 Atuação Cibernética Política/Estratégica - a atuação cibernética política/estratégica ocorre desde o tempo de paz, para atingir um objetivo político ou estratégico definido no mais alto nível, normalmente no contexto de uma Operação de Informação ou de Inteligência, contra ameaças à Segurança Nacional, definidas por autoridades competentes.

2.8.3 Atuação Cibernética Operacional/Tática - a atuação cibernética operacional/tática é tipicamente empregada no contexto de uma Operação Militar, contribuindo para a obtenção de um efeito desejado definido durante o planejamento operacional de uma Hipótese de Emprego (HE).

2.9 Tipos de Ações Cibernéticas

2.9.1 Os tipos de ações cibernéticas são os seguintes:

a) Ataque Cibernético;
b) Exploração Cibernética; e
c) Proteção Cibernética.

2.9.2 Ataque Cibernético – ação sobre dispositivos, redes de computadores e comunicações do oponente para causar os seguintes efeitos cinéticos e não-cinéticos, dentre outros:

a) destruir ou degradar equipamentos e sistemas, provocando baixas e/ou danos permanentes ou temporários, que sejam favoráveis à operação;

b) degradar a capacidade de operação do oponente, reduzindo a eficácia de funcionamento dos seus sistemas;

c) corromper dados de sistemas do oponente, manipulando informações de interesse do TO/A Op;

d) negar o acesso do oponente a sistemas de interesse do TO/A Op; e

e) interromper o funcionamento de sistemas do oponente que tragam vantagem ao TO/A Op.

2.9.3 O ataque cibernético é uma ação não cinética, executado como parte de uma operação militar que abrange as dimensões física e informacional. As ações devem ser coordenadas e sincronizadas com os fogos planejados para os domínios físicos.

2.9.4 Exploração Cibernética – consiste em ações destinadas a mapear sistemas e ativos de informação presentes no espaço cibernético de Interesse, identificar vulnerabilidades e realizar a preparação para futuras ações ofensivas.

2.9.5 As ações exploratórias não-intrusivas incluem atividades de coleta de informação sem o comprometimento do sistema alvo.

2.9.6 As ações exploratórias intrusivas incluem atividades para obter dados negados e apoiar a preparação do ambiente operacional.

2.9.7 Proteção Cibernética - ações para garantir o funcionamento dos dispositivos computacionais, bem como prover a proteção contra ações de exploração e ataque do oponente. É uma atividade de caráter permanente.

2.9.8 Todas as ações cibernéticas podem ser empregadas independentemente do tipo de Operação Cibernética realizada, seja ela Op Ciber Def ou Op Ciber Ofs. Há situações em que ações exploratórias intrusivas e ataques cibernéticos são executados no âmbito de uma Op Ciber Def.

CAPÍTULO III

SISTEMA MILITAR DE DEFESA CIBERNÉTICA

3.1 Considerações Iniciais

3.1.1 A Defesa Cibernética, por ser um dos componentes da Defesa Nacional, é missão das Forças Armadas (FA), conforme a legislação referenciada no Capítulo I. Entretanto, as peculiaridades do espaço cibernético tornam impraticável o cumprimento dessa missão se não houver o comprometimento da sociedade como um todo, imbuída do sentimento de responsabilidade individual e coletiva pela proteção dos sistemas de interesse naquele ambiente.

3.1.2 A eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. Nesse contexto, avulta de importância a necessidade de interação permanente entre o MD e os demais atores externos envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a END.

3.1.3 As atividades de Defesa Cibernética no MD são orientadas para atender às necessidades da Defesa Nacional. A integração com órgãos de interesse deve ser buscada desde a situação de normalidade institucional, com a finalidade de facilitar as ações decorrentes de uma evolução para situações de crise ou conflitos, levando em consideração o amplo espectro desses eventos.

3.1.4 O SMDC é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses.

3.1.5 Cabe também ao SMDC assegurar a proteção cibernética do Sistema Militar de Comando e Controle (SISMC[2]), possibilitando a capacidade de atuar em rede com segurança, bem como de maneira integrada e colaborativa na gestão de riscos que envolvam a proteção de infraestruturas críticas, conforme previsto no Plano Nacional de Segurança de Infraestruturas Críticas.

3.2 Níveis de Decisão

3.2.1. No contexto do SMDC, os níveis de decisão são os seguintes:

a) Nível Político: nível externo que interage com o SMDC, coordenado pelo GSI/PR e abrange a Administração Pública Federal (APF) e as IC. Neste nível, denominado de Segurança Cibernética, o principal ator no que se refere ao Setor Cibernético é o GSI-PR, preponderando as atividades de proteção cibernética. O SMDC relaciona-se com este nível colaborando, por meio de cooperação e integração, com a proteção cibernética das infraestruturas críticas de interesse da Defesa Nacional. O ComDCiber também representa a Defesa na articulação com o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, como equipe de coordenação setorial;

b) Nível Estratégico – nível denominado de Defesa Cibernética e que fica a cargo do MD, do Estado-Maior Conjunto das Forças Armadas e dos Comandos das FA, interagindo com o GSI/PR, APF, agências e IC de interesse para a Defesa Nacional. Neste nível, o Ministério da Defesa e os Comandos das Forças assumem o protagonismo das ações, atuando o ComDCiber como órgão central do SMDC. O principal interlocutor do ComDCiber no Ministério da Defesa é o EMCFA. A partir do nível estratégico, observa-se a mudança do viés exclusivo de segurança cibernética para a defesa cibernética. Embora medidas de segurança sejam implementadas em todos os níveis, a defesa implica que, além da proteção, a exploração e o ataque são executados neste nível, em cumprimento às demandas das autoridades competentes;

c) Nível Operacional – nível denominado de Guerra Cibernética e que fica a cargo dos Comandos Operacionais ativados. Neste nível, uma vez ativado um Comando Operacional, o ComDCiber atuará em ações específicas, por solicitação e em apoio aos Comandos ativados, disponibilizando militares para compor a Subseção de Guerra Cibernética (SGC) da Seção de Operações do Estado-Maior do Comando Ativado, ou solicitando o reforço de especialistas das FA. No nível operacional são realizados o planejamento das ações de proteção, exploração e ataque, com a finalidade de cumprir as demandas dos Comandos ativados; e

d) Nível Tático – nível denominado de Guerra Cibernética e que fica a cargo das Forças Componentes. O nível tático é caracterizado pela ação da Força Conjunta de Guerra Cibernética (F Cj G Ciber) ou de um Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber), além das estruturas de Guerra Cibernética das Forças Componentes. Neste nível ocorre a execução do planejamento tático, onde uma Força Conjunta de Guerra Cibernética atua no cumprimento ao que foi planejado no nível operacional.

3.3 A Estruturação do Sistema Militar de Defesa Cibernética (SMDC)

3.3.1 O ComDCiber é o órgão responsável por assessorar o Ministro de Estado da Defesa na implantação e na gestão do SMDC, com a finalidade de garantir, no âmbito da Defesa Nacional, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança necessários.

3.3.2 A estruturação geral do SMDC pode ser vista abaixo e conta com a participação de militares das FA e civis.
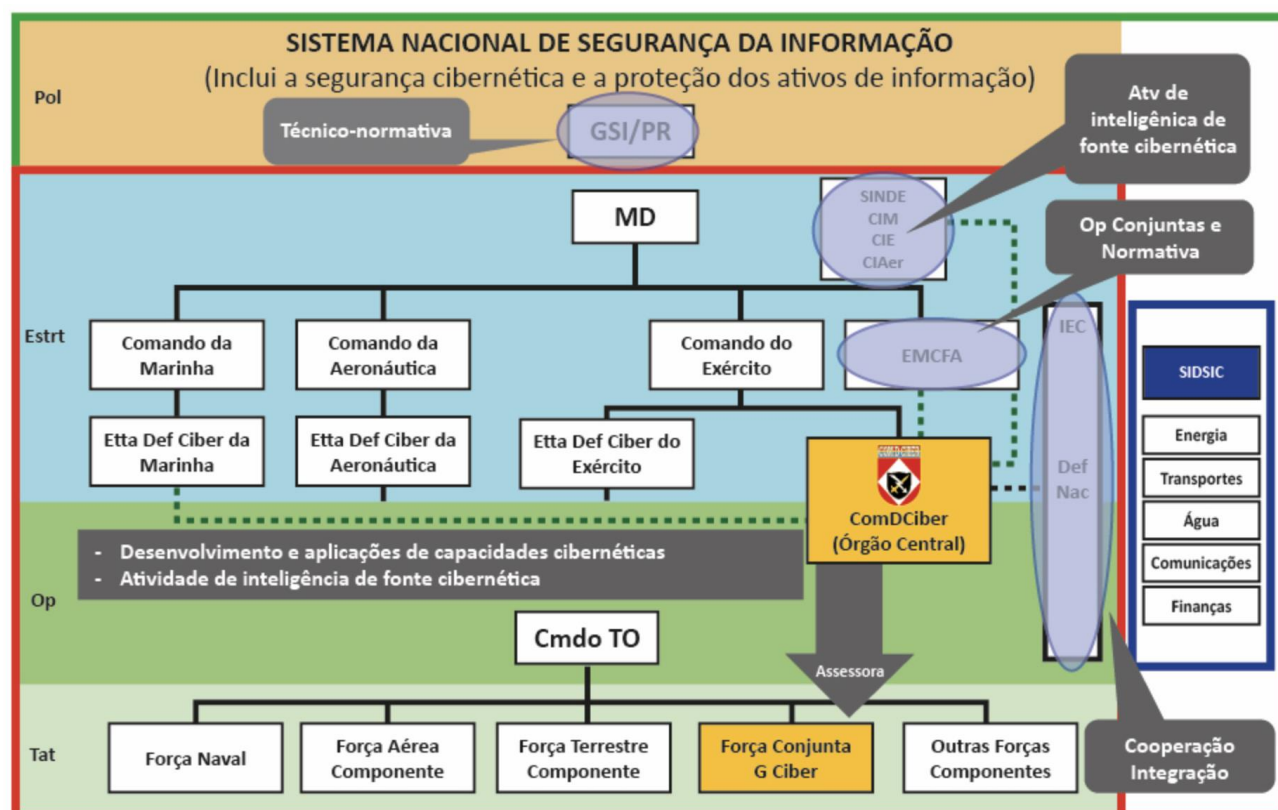
Figura 3 – Sistema Militar de Defesa Cibernética (SMDC)

3.3.3 O órgão central do SMDC é o ComDCiber, comando operacional conjunto, permanentemente ativado e com capacidade interagências. O ComDCiber poderá passar ao controle do MD, por intermédio do EMCFA, nas Operações Conjuntas e conta, permanentemente, com um Centro de Coordenação de Operações Cibernéticas (CCOC) para realizar o planejamento e o controle das ações planejadas no nível estratégico, predominantemente fora do TO, da ZD e da Área de Operações, levando em conta as particularidades de cada FA, de modo a obter uma atuação sinérgica.

3.3.4 O ComDCiber atua no nível estratégico, sob orientação e supervisão do MD, por intermédio do EMCFA, realizando as ações de coordenação e integração do Setor Cibernético nas FA e privilegiando, sempre que possível, uma forma de emprego conjunta.

3.3.5 É responsabilidade de cada FA a adoção de medidas de proteção cibernética dos seus ativos de informação.

3.3.6 O ComDCiber mantém canal técnico para coordenação e integração com os órgãos de interesse envolvidos nas atividades de Defesa Cibernética (CERT.br, CTIR Gov, órgãos de Defesa/Guerra Cibernética das FA, Ministérios, Agências Governamentais, dentre outros).

3.3.7 O ComDCiber mantém canal sistêmico/técnico com os órgãos centrais de inteligência das FA, no âmbito do Sistema de Inteligência de Defesa (SINDE), no tocante ao Setor Cibernético, para a difusão e obtenção dos dados obtidos por intermédio da Fonte Cibernética.

3.3.8 A F Cj G Ciber ou o Dst Cj G Ciber mantém canal técnico com as Estruturas de Guerra Cibernética das demais Forças Componentes (F Cte), no âmbito do Comando Operacional Ativado, e com o ComDCiber. Por esse canal, recebe assessoramento no tocante às ações de Guerra Cibernética, para a difusão e obtenção dos dados necessários às operações.

3.3.9 As Estruturas de Guerra Cibernética das F Cte devem garantir a capacidade de proteção cibernética dos seus ativos de informação desdobrados.

3.4 Nível de Alerta Cibernético

3.4.1 Entende-se por Nível de Alerta Cibernético, para emprego no âmbito do MD e das FA, tanto em operações conjuntas quanto nas atividades diárias, a classificação dada ao estado em que se encontra o Espaço Cibernético de Interesse do MD e das FA, no tocante à possibilidade de atuação das ameaças cibernéticas.

3.4.2 Trata-se de uma escala progressiva do grau do risco de ocorrência de ataques cibernéticos, concebida para orientar a coordenação das ações de proteção do espaço cibernético do SMDC. A elevação do alerta cibernético sinaliza a possibilidade de escalar as ações de proteção, visando a neutralizar ou impedir o efeito desejado das ameaças identificadas.

3.4.3 Para o estabelecimento dos níveis de alerta cibernético, são considerados os seguintes fatores:

a) a probabilidade de atuação das ameaças cibernéticas no espaço cibernético do SMDC;

b) a interpretação de cada nível de alerta está associada a um ou mais cenários de riscos, os quais podem ser hipotéticos, advindos de lições aprendidas obtidas em exercícios simulados, missões reais ou pelo histórico de eventos ocorridos;

c) a mudança de um nível para outro pode ser ou não sequencial, ou seja, existe a possibilidade de mudanças entre níveis não sucessivos, saltando-se níveis intermediários; e

d) a variação de um nível para outro está associada a uma ou mais das seguintes condições:

1) mudança da probabilidade de ocorrência das ameaças existentes, segundo os critérios de análise de riscos adotados;

2) concretização de ameaças existentes; e

3) abrangência do impacto da concretização de ameaças, segundo os critérios de análise de risco adotados.

3.4.4 Cada nível de alerta demanda um conjunto de procedimentos correspondentes, os quais devem atender as especificidades de cada FA ou serem próprios para o emprego pelo SMDC, nas atividades diárias ou em Operações Conjuntas. Estes procedimentos devem ser explicitados no planejamento da operação ou em publicações pertinentes.

3.4.5 Cada nível é designado por uma cor e por um nome que evocam o grau de risco correspondente à possibilidade de concretização de ameaças cibernéticas no Espaço Cibernético de Interesse do SMDC.

3.4.6 Os níveis de alerta cibernético, para emprego no âmbito do SMDC com seus respectivos significados e/ou interpretações, são os seguintes:

Nível de Alerta		Significado / Interpretação (*)
Cor	Nome	
Verde	Baixo	a) aplicável quando as ameaças cibernéticas percebidas não afetam o Espaço Cibernético de Interesse do SMDC, situação normal ou rotineira; b) a probabilidade de concretização de ameaças cibernéticas é muito baixa, considerando o histórico; c) risco baixo de incidente de segurança; e d) nenhuma evidência de atividade incomum, além da preocupação normal com as atividades cibernéticas conhecidas.
Azul	Moderado	a) aplicável quando as ameaças cibernéticas percebidas afetam o Espaço Cibernético de Interesse do SMDC, sem comprometer as infraestruturas críticas de interesse da Defesa Nacional; b) a probabilidade de concretização de ameaças cibernéticas encontra-se entre baixa e moderada, considerando o histórico de ameaças; c) risco moderado de incidentes de segurança, em função do aumento das atividades cibernéticas maliciosas acima dos níveis normais ou rotineiros; e d) existem evidências de atividades cibernéticas maliciosas, mas sem um incidente conhecido ou com um incidente conhecido sem impacto significativo.
Amarelo	Médio	a) aplicável quando forem identificadas ações cibernéticas hostis que afetam o Espaço Cibernético de Interesse do SMDC, existe a percepção de ameaças cibernéticas contra as infraestruturas críticas de interesse da Defesa Nacional, porém não existindo o comprometimento; b) a probabilidade da concretização de ameaças cibernéticas encontra-se entre moderada e média, considerando o histórico; c) risco médio de incidentes de segurança, em função do aumento das atividades cibernéticas maliciosas acima do nível moderado; e d) há vulnerabilidades conhecidas que estão sendo exploradas causando danos, interrupções ou indisponibilidade de ativos com impacto moderado ou com a probabilidade de um alto potencial de impacto significativo.
Laranja	Alto	a) aplicável quando forem identificadas ações cibernéticas hostis que degradam alguma infraestrutura crítica de interesse da Defesa Nacional, porém com a possibilidade de restabelecimento das condições de segurança ou dos serviços em tempos aceitáveis para o cumprimento da missão; b) a probabilidade de concretização de ameaças cibernéticas

		encontra-se entre média e alta, considerando o histórico; c) risco alto de incidentes de segurança, em função do comprometimento de infraestrutura crítica de interesse da Defesa Nacional por atividades maliciosas, causando várias interrupções de serviço críticos ou vários comprometimentos de ativos críticos; e d) as vulnerabilidades exploradas possuem um alto impacto causando danos, interrupções ou indisponibilidades.
Vermelho	**Severo**	a) aplicável quando as ações cibernéticas hostis degradam alguma infraestrutura crítica de interesse da Defesa Nacional, porém com possibilidade de restabelecimento das condições de segurança ou dos serviços em tempos além dos aceitáveis para o cumprimento da missão; b) existe a concretização de ameaças cibernéticas; c) atividades maliciosas, com graves impactos, resultando em interrupções generalizadas ou comprometimentos destrutivos significativos para sistemas sem solução conhecida ou em ativos de infraestrutura crítica; e d) as vulnerabilidades estão sendo exploradas causando impactos graves nas infraestruturas críticas de interesse da Defesa Nacional com interrupções ou indisponibilidades de serviços.

(*) Observação: as ações a serem adotadas em cada nível de alerta serão detalhadas nas Normas Operacionais do Sistema Militar de Defesa Cibernética (NOSDCIBER).

3.4.7 Durante as operações conjuntas, cabe ao Chefe do EMCFA, ainda, ratificar o nível de alerta cibernético proposto pelo Cmt TO/A Op, com o assessoramento do ComDCiber, tendo em vista o TO estar incluso no Espaço Cibernético de Interesse do SMDC.

3.4.8 O nível de alerta cibernético de cada FA não deverá ser inferior ao nível de alerta cibernético adotado para o SMDC.

CAPÍTULO IV

COMANDO DE DEFESA CIBERNÉTICA

4.1 Considerações Iniciais

4.1.1 O ComDCiber é um Comando Operacional Conjunto, permanentemente ativado e com capacidade interagências, pertencente à estrutura regimental do Exército Brasileiro. Tem como missão, respeitadas as competências das FA e dos Comandos Operacionais ativados: planejar; orientar; coordenar; integrar; e executar atividades relacionadas ao desenvolvimento e à aplicação das capacidades cibernéticas, como órgão central e no âmbito do SMDC, a fim de contribuir para o uso efetivo do espaço cibernético, impedindo ou dificultando sua utilização contra os interesses da Defesa Nacional.

4.1.2 Desde a situação de normalidade, o ComDCiber, em ligação com o SINDE, com o Sistema de Inteligência Operacional (SIOP), com o Sistema Militar de Comando e Controle ($SISMC^2$), com as estruturas cibernéticas das FA e com outras estruturas do SMDC, coordena operações cibernéticas que compreendem: a proteção dos ativos de informação do MD e das FA e o levantamento de dados para estruturação e atualização do banco de dados estratégico sobre as ameaças cibernéticas; a colaboração com a proteção cibernética de infraestruturas críticas de interesse da Defesa; e a execução de outras ações cibernéticas.

4.1.3 O ComDCiber participa da elaboração dos Planos Estratégicos de Emprego Conjunto das Forças Armadas (PEECFA), exerce as funções normais de Estado-Maior do Comando de Defesa Cibernética em operações e, ainda, cede pessoal para mobiliar as estruturas de defesa cibernética dos demais Comandos Operacionais ativados e do Comando e Estado-Maior da Força Conjunta de Guerra Cibernética, quando constituída.

4.2 Competências do ComDCiber

a) colaborar com o GSI/PR e os órgãos da APF nos assuntos relacionados à Segurança Cibernética para a proteção das IC de interesse da Defesa por meio da cooperação e integração de esforços;
b) assessorar o MD e os Comandos das Forças Armadas nos assuntos relacionados às atividades do Setor Cibernético da Defesa;
c) elaborar e propor ao MD, por intermédio do EMCFA, arcabouço normativo do SMDC.
d) Contribuir para a proteção cibernética dos sistemas de interesse da Defesa, definidos pelo MD;
e) manter canal sistêmico e técnico com os órgãos centrais de Inteligência das FA, no âmbito do SINDE, no tocante ao Setor Cibernético;
f) fomentar a pesquisa, o desenvolvimento e a inovação das capacidades cibernéticas de interesse da Defesa;
g) assessorar o EMCFA no trato da Sistemática de Planejamento de Emprego Conjunto das Forças Armadas (SisPECFA), nos planejamentos relacionados ao emprego da Defesa e da Guerra Cibernética;

h) propor e executar ações colaborativas com nações amigas no Setor Cibernético da Defesa;
i) planejar, orientar, coordenar e integrar atividades relacionadas ao desenvolvimento e aplicação das capacidades cibernéticas, no âmbito do SMDC, respeitadas as competências das FA e dos Comandos Operacionais ativados, a fim de contribuir para o uso efetivo do espaço cibernético, impedindo ou dificultando sua utilização contra os interesses da Defesa Nacional;
j) executar ações cibernéticas em situações de paz, crise ou conflito armado, no domínio operacional cibernético, respeitadas as competências das FA e dos Comandos Operacionais ativados; e
k) promover e fomentar o incremento e aperfeiçoamento das capacidades cibernéticas no âmbito do SMDC.

4.3 Estrutura do ComDCiber

4.3.1 O Comando de Defesa Cibernética possui a seguinte estrutura:
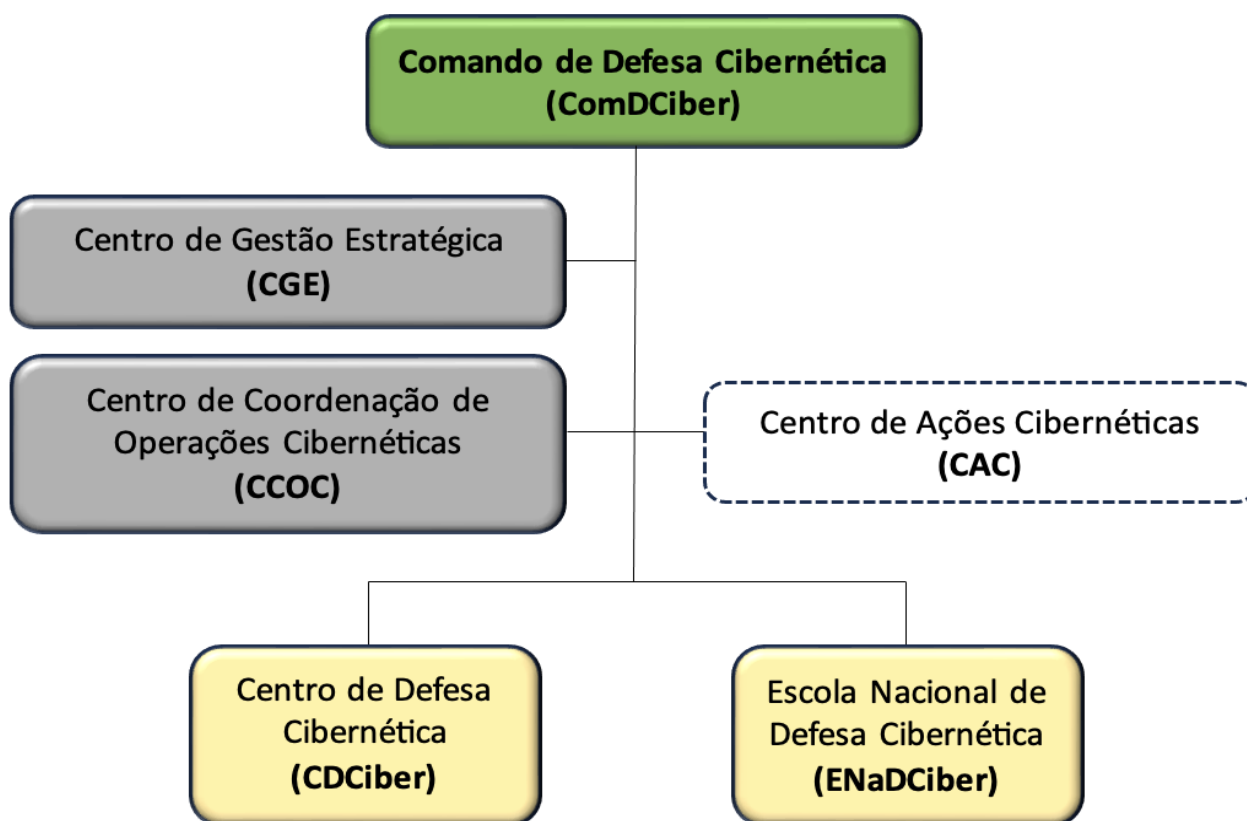
Figura 4 – Estrutura do ComDCiber

4.3.2. Para cumprir suas missões operativas e de gestão estratégica, o ComDCiber é assim constituído:

a) Centro de Coordenação de Operações Cibernéticas (CCOC): tem como tarefas aplicar as capacidades cibernéticas, no âmbito do SMDC, realizando o planejamento das operações conjuntas, combinadas e interagências;

b) Centro de Ações Cibernéticas (CAC): tem como tarefas executar as operações de Defesa e Guerra Cibernéticas, observando as técnicas, táticas e procedimentos específicos. Atualmente esta função é exercida pelo Centro de Defesa Cibernética (CDCiber).

c) Centro de Gestão Estratégica (CGE): tem como tarefa coordenar os processos afetos ao Planejamento, Gestão Estratégica, Relações Institucionais, Gestão do Conhecimento e de Talentos no âmbito do ComDCiber; e

d) Escola Nacional de Defesa Cibernética (ENaDCiber): tem como tarefa capacitar recursos humanos para o setor cibernético da Defesa Nacional.

CAPÍTULO V

CAPACIDADE CIBERNÉTICA EM OPERAÇÕES

5.1 Considerações Iniciais

5.1.1 O Setor Cibernético nacional envolve a atuação integrada de vários órgãos, sejam civis ou militares, cada um com atribuições específicas, tornando mais provável o emprego em ambiente interagências.

5.1.2. Em qualquer operação militar que envolva o componente cibernético, a cooperação e o intercâmbio de informações são fatores essenciais para uma atuação efetiva. Esses aspectos tornam essencial o estabelecimento e/ou o fortalecimento de parcerias estratégicas com órgãos de Segurança e/ou Defesa Cibernética nacionais e internacionais.

5.1.3 A capacidade cibernética constitui um atuador não cinético e multiplicador do poder de combate, pela possibilidade de causar efeitos cinéticos e não cinéticos, podendo contribuir para causar, inclusive, um efeito de paralisia estratégica, operacional ou tática no oponente.

5.1.4 A efetividade da Guerra Cibernética depende de abrangente e prévia atividade de preparação do ambiente operacional, caracterizada por intensas ações de exploração cibernética, realizadas desde a situação de normalidade.

5.2 Concepção do Planejamento e Emprego da Capacidade Cibernética em Operações
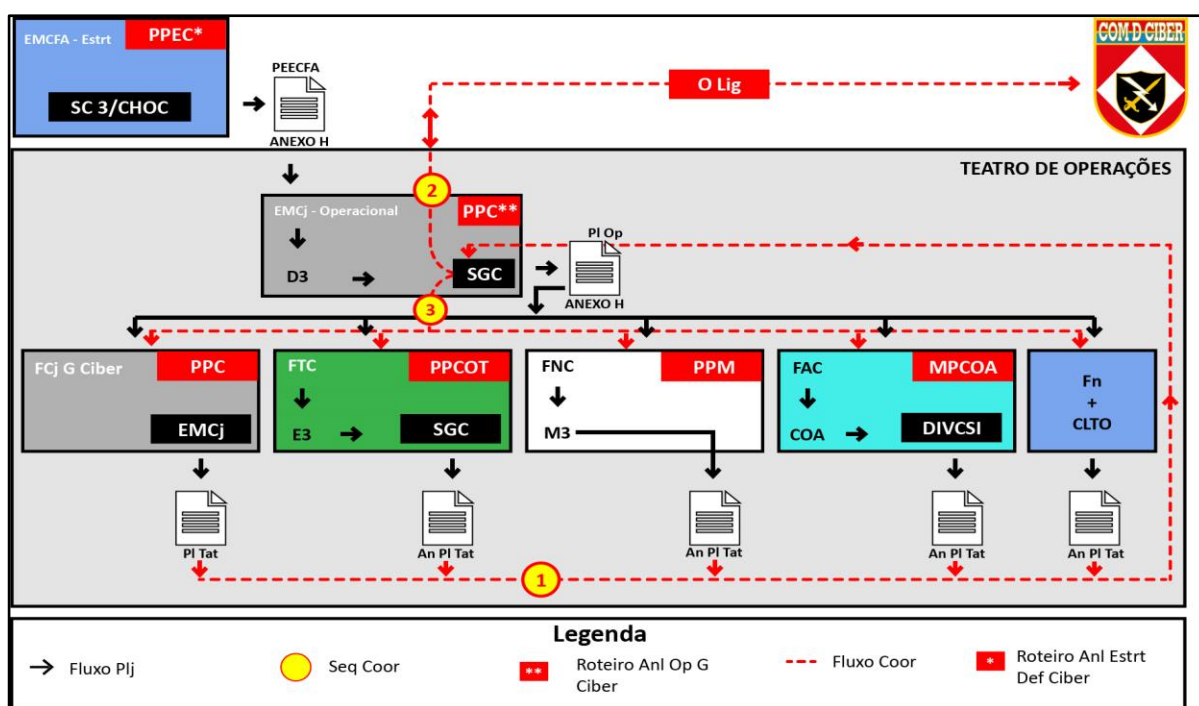
Figura 5 – Fluxo de Planejamento e Coordenação da Capacidade Cibernética em Operações.

5.2.1 O planejamento da Capacidade Cibernética nas operações deve ter início por ocasião do Levantamento Estratégico de Área (LEA), conduzindo ao Exame de Situação Estratégico de uma Hipótese de Emprego (HE), e da elaboração do PEECFA, com seu respectivo Anexo de Defesa Cibernética.

5.2.2 Os PEECFA deverão considerar o vulto da Capacidade Cibernética a ser empregada, bem como as ameaças e a análise de risco cibernético para consecução dos objetivos estabelecidos.

5.2.3 Para o planejamento, no nível operacional em situação de guerra e não-guerra, a SGC, que faz parte da estrutura da Seção de Operações (D-3), deverá produzir o Anexo de Guerra Cibernética ao Plano Operacional.

5.2.4 Para o planejamento, no nível tático em situação de guerra e não-guerra, a F Cj G Ciber ou Dst Cj G Ciber, respectivamente, deverá produzir o Plano Tático de Guerra Cibernética com seus anexos, alinhados ao Anexo de Guerra Cibernética do Plano Operacional, assim como as F Cte seus anexos de G Ciber aos seus Planos Táticos.

5.2.5 O ComDCiber, em seu emprego operativo, atua no nível estratégico e, excepcionalmente, pode também atuar nos níveis operacional e tático do TO/A Op, quando não constituída uma F Cj G Ciber ou Dst Cj G Ciber, com o objetivo de assegurar o uso efetivo do espaço cibernético pelas Forças Armadas e pelos Comandos Operacionais ativados e impedir ou dificultar sua utilização contra interesses da Defesa Nacional.

5.2.6 A participação do ComDCiber deverá ocorrer em todas as operações, uma vez que a transversalidade e a ausência de limites físicos, tornando possível, em qualquer situação, a necessidade de ação cibernética sobre alvos localizados fora do TO/A Op.

5.2.7 O ComDCiber assessora o Cmdo TO/A Op na adjudicação dos meios/pessoal para organização da F Cj G Ciber. Cabe ressaltar que não existe subordinação da F Cj G Ciber para com o ComDCiber durante as operações.

5.2.8 O desdobramento de uma F Cj G Ciber no TO/A Op é definido durante o planejamento operacional do Com TO/A Op. As ações cibernéticas, fora do TO são de responsabilidade do ComDCiber.

5.2.9 O planejamento do emprego da capacidade cibernética dentro do TO/A Op é realizado pela SGC, que faz parte da estrutura da Seção de Operações do Estado-Maior (D-3) do Cmdo TO/A Op, conforme definido no manual MD30-M-01/Doutrina de Operações Conjuntas.

5.2.10 Tendo em vista a característica de o espaço cibernético não estar restrito aos limites físicos, o Cmdo TO/A Op possui um canal técnico com o ComDCiber, por meio da SGC, a fim de coordenar as ações visando aos efeitos desejados e evitando os efeitos colaterais.

5.2.11 Nas situações de emprego, o ComDCiber utilizará seus meios orgânicos e adjudicados.

5.2.12 Nas situações de emprego em que não for ativado um Comando Operacional, poderá ser constituído 1 (um) Dst Cj G Ciber em apoio à operação.

5.2.13 Poderá ser adjudicado ao Comando Operacional ativado, em situações de não-guerra, 01 (um) Dst Cj G Ciber, diretamente subordinado ao referido Comando Operacional, integrando suas tropas.

5.2.14 A coordenação do emprego da capacidade cibernética inicia com o recebimento pela SGC do Plano Tático da F Cj G Ciber e dos anexos de G Ciber oriundos das demais F Cte. De posse desses documentos, a SGC verifica a adequação entre as ações previstas em comparação ao previsto no Anexo de G Ciber ao Plano Operacional, verificando redundâncias, necessidades de ações, meios ou especialidades adicionais a serem coordenados com o ComDCiber, dentro do próprio EM Cj e com as F Cte, finalizando o ciclo de coordenação dentro do TO.

5.3 A Capacidade Cibernética em proveito da Inteligência

5.3.1 A Exploração Cibernética e a Inteligência Cibernética compartilham das mesmas táticas, técnicas e procedimentos e visam preparar o espaço cibernético para Op Ciber futuras.

5.3.2. A integração das diferentes fontes de Inteligência (humanas, imagens, sinais, cibernética e outras) para a produção de conhecimento é, normalmente, realizada nos sistemas de Inteligência do MD e das FA.

5.3.3. O ComDCiber e os órgãos de Defesa Cibernética das FA podem produzir conhecimento oriundo exclusivamente da Fonte Cibernética, como também podem empregar conhecimento de outras fontes para melhor desempenhar suas funções.

5.3.4. As ações de Exploração Cibernética, além de se constituírem como ferramentas importantes para o mapeamento do Espaço Cibernético de Interesse, também, são pertinentes ao ramo de Inteligência, atividade prevista na Lei Complementar nº 97, de 9 de junho de 1999 e posteriores alterações.

ANEXO

SIGLAS, ABREVIATURAS E ACRÔNIMOS

As siglas, abreviaturas e acrônimos abaixo aplicam-se a este documento, tendo em vista não constarem no Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas – MD33-M-02 (4ª edição/2021) ou por terem outro significado naquele manual.

ABREVIATURA	SIGNIFICADO
Aç Rsp	Ações de Resposta
APF	Administração Pública Federal
CDCiber	Centro de Defesa Cibernética
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CG Ciber	Centro de Gravidade Cibernético
ComDCiber	Comando de Defesa Cibernética
CTIR.Gov	Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo
DIVCSI	Divisão de Comunicação e Sistemas de Informação
Dst Cj G Ciber	Destacamento Conjunto de Guerra Cibernética
E-Ciber	Estratégia Nacional de Segurança Cibernética
ENaDCiber	Escola Nacional de Defesa Cibernética
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
MDI	Medidas de Defesa Interna
MPCOA	Manual de Planejamento e Condução de Operações Aeroespaciais
Op Ciber	Operações Cibernéticas
Op Ciber Def	Operações Cibernéticas Defensivas
Op Ciber Ofs	Operações Cibernéticas Ofensivas
PDCDN	Programa Defesa Cibernética na Defesa Nacional
PNSI	Política Nacional de Segurança da Informação
PNSIC	Plano Nacional de Segurança de Infraestruturas Críticas
PPCOT	Processo de Planejamento e Condução das Operações Terrestres

Ministério da Defesa
Estado-Maior Conjunto das Forças Armadas
Brasília, 25 de outubro de 2023.